HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 80527-2400

PATENT APPLICATION

ATTORNEY DOCKET NO. 200310181-1

IN THE
UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s):	Eric M. PETERSON et al.	Confirmation No.:	5440
Application No.:	10/691,262	Examiner:	Michael E. Keefer
Filing Date:	October 22, 2003	Group Art Unit:	2454

Title: SYSTEM AND METHOD OF NETWORK USAGE ANALYZER

Mail Stop Appeal Brief-Patents
Commissioner For Patents
PO Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF

Transmitted herewith is the Appeal Brief in this application with respect to the Notice of Appeal filed on July 2, 2009.

☒ The fee for filing this Appeal Brief is $540.00 (37 CFR 41.20).

□ No Additional Fee Required.

(complete (a) or (b) as applicable)

The proceedings herein are for a patent application and the provisions of 37 CFR 1.136(a) apply.

□ (a) Applicant petitions for an extension of time under 37 CFR 1.136 (fees: 37 CFR 1.17(a)-(d)) for the total number of months checked below:

□ 1st Month $130 □ 2nd Month $490 □ 3rd Month $1110 □ 4th Month $1730

□ The extension fee has already been filed in this application.

☒ (b) Applicant believes that no extension of time is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

Please charge to Deposit Account 08-2025 the sum of $ 540 . At any time during the pendency of this application, please charge any fees required or credit any over payment to Deposit Account 08-2025 pursuant to 37 CFR 1.25. Additionally please charge any fees to Deposit Account 08-2025 under 37 CFR 1.16 through 1.21 inclusive, and any other sections in Title 37 of the Code of Federal Regulations that may regulate fees.

Respectfully submitted,
Eric M. PETERSON et al.
By:
Timothy B. Kang
Attorney/Agent for Applicant(s)
Reg No. : 46,423
Date : July 2, 2009
Telephone : 703-652-3817

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 80527-2400

PATENT APPLICATION

ATTORNEY DOCKET NO. 200310181-1

IN THE
UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s): Eric M. PETERSON et al.

Confirmation No.: 5440

Application No.: 10/691,262

Examiner: Michael E. Keefer

Filing Date: October 22, 2003

Group Art Unit: 2454

Title: SYSTEM AND METHOD OF NETWORK USAGE ANALYZER

Mail Stop Appeal Brief-Patents
Commissioner For Patents
PO Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF

Transmitted herewith is the Appeal Brief in this application with respect to the Notice of Appeal filed on July 2, 2009.

☒ The fee for filing this Appeal Brief is $540.00 (37 CFR 41.20).

☐ No Additional Fee Required.

(complete (a) or (b) as applicable)

The proceedings herein are for a patent application and the provisions of 37 CFR 1.136(a) apply.

☐(a) Applicant petitions for an extension of time under 37 CFR 1.136 (fees: 37 CFR 1.17(a)-(d)) for the total number of months checked below:

☐ 1st Month $130 ☐ 2nd Month $490 ☐ 3rd Month $1110 ☐ 4th Month $1730

☐ The extension fee has already been filed in this application.

☒(b) Applicant believes that no extension of time is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

Please charge to Deposit Account 08-2025 the sum of $ 540. At any time during the pendency of this application, please charge any fees required or credit any over payment to Deposit Account 08-2025 pursuant to 37 CFR 1.25. Additionally please charge any fees to Deposit Account 08-2025 under 37 CFR 1.16 through 1.21 inclusive, and any other sections in Title 37 of the Code of Federal Regulations that may regulate fees.

Respectfully submitted,

Eric M. PETERSON et al.

By:

Timothy B. Kang

Attorney/Agent for Applicant(s)

Reg No. : 46,423

Date : July 2, 2009

Telephone : 703-652-3817

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 80527-2400

Attorney Docket No.: 200310181-1

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s):	Eric M. PETERSON et al.	**Confirmation No.:**	5440
Serial No.:	10/691,262	**Examiner:**	Michael E. Keefer
Filed:	October 22, 2003	**Group Art Unit:**	2454

Title: SYSTEM AND METHOD OF NETWORK USAGE ANALYZER

MAIL STOP APPEAL BRIEF - PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF - PATENTS

Sir:

This is an Appeal Brief in connection with the decisions of the Examiner in a Final Office Action mailed April 3, 2009, and in connection with the Notice of Appeal filed herewith. It is respectfully submitted that the present application has been more than twice rejected. Each of the topics required in an Appeal Brief and a Table of Contents are presented herewith and labeled appropriately.

TABLE OF CONTENTS

(1) Real Party in Interest

The real party in interest is Hewlett-Packard Development Company, L.P.

(2) Related Appeals and Interferences

The Appellant is unaware of any appeals or interferences related to this case.

(3) Status of Claims

Claims 1-3, 6-8, 10-13 and 16-20 are pending in the present application of which claims 1, 6, and 12 are independent. Claims 1-3, 6-8, 10-13 and 16-20 are all rejected and are all appealed.

(4) Status of Amendments

No amendment was filed subsequent to the Final Office Action dated April 3, 2009.

(5) Summary of Claimed Subject Matter

Independent claims 1, 6 and 12 are the claims that are argued together in this appeal. It should be understood that the citations below to the original disclosure as providing support for the claimed features are merely exemplary and do not limit the claimed features to only those citations.

Claim 1. A network usage analyzer (Fig. 1), comprising:

a network query client (14) residing in a first network (18); and

a network query server (12) residing in a second network (16) protected by a firewall (20), wherein said network query client is configured to send authenticating information to the network query server (34 in Fig. 2, paragraph [0015]), to send a query to the network query server related to how resources in the second network are used (40 in Fig. 2, paragraph [0015]), wherein the network query server is configured to send authentication approval information to the network query client (36 in Fig. 2, paragraph [0015]), to collect data related to how resources in the second network are used (paragraph [0016]), and to send collected data to the network query client (44 in Fig. 2, paragraph [0016]) and wherein at least one query is formatted to enable transmission using Hypertext Transfer Protocol (HTTP) as the underlying transport mechanism (paragraphs [0014] and [0016]).

Claim 6. A method for accessing information of resource usage in a first network (Fig. 2), comprising:

establishing a communication channel between a network query client residing in a second network and a network query server residing in the first network protected by a firewall (32 in Fig. 2, paragraph [0015]);

sending, by the network query client, authenticating information to the network query server (34 in Fig. 2, paragraph [0015]);

sending, by the network query server, authentication approval information to the network query client (36 in Fig. 2, paragraph [0015]);

sending, by the network query client, at least one network usage query (40 in Fig. 2, paragraph [0015]);

receiving, by the network query server, at least one network usage query from the network query client, the at least one query formatted to enable transmission using Hypertext Transfer Protocol (HTTP) as the underlying transport mechanism (42 in Fig. 2, paragraph [0016]);

collecting, by the network query server, information requested by the network usage query (paragraph [0016]); and

sending, by the network query server, the collected information to the network query client (44 in Fig. 2, paragraph [0016]).

Claim 12. A method for accessing information of resource usage in a first network (Fig. 2), comprising:

establishing a communication channel between a network query client residing in a second network and a network query server residing in the first network protected by a firewall (32 in Fig. 2, paragraph [0015]);

sending, by the network query client, authenticating information to the network query server (34 in Fig. 2, paragraph [0015]);

sending, by the network query server, authentication approval information to the network query client (36 in Fig. 2, paragraph [0015]);

sending, by the network query client, at least one network network configuration query to the network query server, the at least one query formatted to enable transmission using Hypertext Transfer Protocol (HTTP) as the underlying transport mechanism (42 in Fig. 2, paragraph [0016]);

collecting, by the network query server, network configuration information requested by the network usage query (paragraph [0016]);

receiving, by the network query client, information related to the network configuration query collected by the network query server (paragraph [0016]); and

sending, by the network query server, the collected network configuration information to the network query client (44 in Fig. 2, paragraph [0016]).

(6) Grounds of Rejection to be Reviewed on Appeal

A. Claims 1-3, 6-8, 11-13 and 16-20 were rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,279,113 to Vaidya (hereinafter "Vaidya") in view of the article titled "SOAP: The Simple Access Protocol" authored by Skonnard (hereinafter "Skonnard").

B. Claim 10 was rejected under 35 U.S.C. §103(a) as being unpatentable over Vaidya in view of Skonnard, in view of U.S. Patent No. 5,978,478 to Korematsu (hereinafter "Korematsu") and further in view of U.S. Patent Application Publication No. 2002/0049909 to Jackson et al. (hereinafter "Jackson").

(7) Arguments

A. The rejection of claims 1-3, 6-8, 11-13 and 16-20 under 35 U.S.C. §103(a) as being unpatentable over Vaidya in view of Skonnard should be reversed.

The test for determining if a claim is rendered obvious by one or more references for purposes of a rejection under 35 U.S.C. § 103 is set forth in *KSR International Co. v. Teleflex Inc.*, 550 U.S. 398, 82 USPQ2d 1385 (2007):

> "Under §103, the scope and content of the prior art are to be determined; differences between the prior art and the claims at issue are to be ascertained; and the level of ordinary skill in the pertinent art resolved. Against this background the obviousness or nonobviousness of the subject matter is determined. Such secondary considerations as commercial success, long felt but unsolved needs, failure of others, etc., might be utilized to give light to the circumstances surrounding the origin of the subject matter sought to be patented." Quoting *Graham v. John Deere Co. of Kansas City*, 383 U.S. 1 (1966).

According to the Examination Guidelines for Determining Obviousness Under 35 U.S.C. 103 in view of *KSR International Co. v. Teleflex Inc.*, Federal Register, Vol. 72, No. 195, 57526, 57529 (October 10, 2007), once the *Graham* factual inquiries are resolved, there must be a determination of whether the claimed invention would have been obvious to one of ordinary skill in the art based on any one of the following proper rationales:

> (A) Combining prior art elements according to known methods to yield predictable results; (B) Simple substitution of one known element for another to obtain predictable results; (C) Use of known technique to improve similar devices (methods, or products) in the same way; (D) Applying a known technique to a known device (method, or product) ready for improvement to yield predictable results; (E) ''Obvious to try''—choosing from a finite number of identified, predictable solutions, with a reasonable expectation of success; (F) Known work in one field of endeavor may prompt variations of it for use in either the same field or a different one based on design incentives or other market forces if the variations would have been predictable to one of ordinary skill in the art; (G)

> Some teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill to modify the prior art reference or to combine prior art reference teachings to arrive at the claimed invention. *KSR International Co. v. Teleflex Inc.*, 550 U.S. 398, 82 USPQ2d 1385 (2007).

Furthermore, as set forth in *KSR International Co. v. Teleflex Inc.*, quoting from *In re Kahn*, 441 F. 3d 977, 988 (CA Fed. 2006), "[R]ejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasonings with some rational underpinning to support the legal conclusion of obviousness."

Furthermore, as set forth in MPEP 2143.03, to ascertain the differences between the prior art and the claims at issue, "[a]ll claim limitations must be considered" because "all words in a claim must be considered in judging the patentability of that claim against the prior art." *In re Wilson*, 424 F.2d 1382, 1385.

If the above-identified criteria and rationales are not met, then the cited references fail to render obvious the claimed invention and, thus, the claimed invention is distinguishable over the cited references.

Claims 1-3, 6-8, 11-13 and 16-20:

The rejection of claims 1-3, 6-8, 11-13 and 16-20 under 35 U.S.C. §103(a) as being unpatentable over Vaidya in view of Skonnard should be reversed for at least the following reasons.

- The rejection should have been over Vaidya in view of Skonnard and Korematsu:

In the heading, claims 1-3, 6-8, 11-13 and 16-20 were rejected based on Vaidya in view of Skonnard. However, in the body of the rejection, the Office Action also included Korematsu

(See page 4 of the final Office Action). Therefore, it is assumed that the rejection of claims 1-3, 6-8, 11-13 and 16-20 is based on Vaidya in view of Skonnard and Korematsu. The arguments below will be in response to Vaidya in view of Skonnard and Korematsu.

- Arguments:

Independent Claim 1:

Independent claim 1 recites a network query client ("client") in a first network, a network query server ("server") in a second network protected by a firewall, wherein the client is configured to send a query to the server related to how resources in the second network are used, and wherein the server is configured to collect data related to how resources in the second network are used and send that collected data to the client. Support for the query "related to how the resources in the second network are used" can be found at least in paragraph [0015] of the specification of the present application. Vaidya, Skonnard and Korematsu, taken individually or in combination, fail to teach or suggest at least the features recited above.

Vaidya pertains to a method and system for providing security on a communication system against external intrusions. *Vaidya*, col. 1, lines 11-15. The system of Vaidya includes a local area network (LAN) 11 and a remote network 24. *Vaidya*, Fig. 1, col. 5, lines 5-25. The remote network 24 includes network security data to be transmitted and stored in the repository 12 of the LAN 11. Initially, the repository 12 of the LAN 11 polls the network 24 for the security data. *Vaidya*, col. 5, lines 47-50. The network 24 transmits the security data to the repository 12 to be stored. *Vaidya*, col. 5, 39-43. The repository 12 then sends attack signature profiles to the collector 10 of the network 24. *Vaidya*, col. 5, lines 29-33. Attack signature profiles are patterns which constitute known security violations. *Vaidya*, col. 2, lines 35-37. The collector 10 of the network 24 uses the attack signature profiles to determine whether there is an intrusion attempt. If there is an intrusion attempt, the collector 10 can terminate an application session, trace the session and/or alert the network administrator of the attack. *Vaidya*, from col. 6, line 57 to col. 7, line 11.

With such a system, Vaidya fails to teach or suggest that the client is configured to send a query to the server related to how resources in the second network are used, that the server is configured to collect data related to how the resources in the second network are used and send that collected data to the client, as recited in independent claim 1. Instead, Vaidya discloses that the repository 12 polls the data collector 10 in the network 24 to obtain the network security data from the network 24. *Vaidya*, col. 5, lines 26-27. In the rejection, the Examiner asserts that such network security data from the network 24 is the data related to how resources in the second network are used, recited in independent claim 1, because the network security data in Vaidya "do relate to how the resources of that network are being used, i.e. are they being used properly or not." *Final Office Action*, page 6, last sentence. This assertion is respectfully traversed.

In Vaidya, the security data stored in the repository 12 are sensitive material or application that needs to be protected from external intrusions. Thus, at best, the security data from the networks may be called resources of those networks. As such, the security data transmitted from the network 24 to the repository 12 at best may be called the resources of the network 24. However, that security data from the network 24 does not represent how the security data are being used in the network 24. Therefore, when the repository 12 polls the data collector 10 of the network 24 for the security data (Vaidya, col. 5, lines 27-29) , the repository 12 sends a query for the resources of the network 24, but the repository 12 does not send a query for data related to how the resources are being used in the network 24. The repository 12 in Vaidya only has the function of storing the security data of the network 24. The repository 12 does not store any data related to how the security data of the network 24 are being used. In addition, the repository 12 uses the security data to determine whether there have been unauthorized access into the network 11. Thus, the security data in Vaidya is concerned only with unauthorized access to the resources in the network, but not with how the resources are being used in the network. Accordingly, Vaidya fails to teach or suggest the query related how resources in the second network are being used, as recited in independent claim 1.

In addition to lacking the feature discussed above, Vaidya also fails to teach or suggest a server in a second network protected by a firewall, as recited in independent claim 1. As stated above, claim 1 recites a client in a first network and a server in a second network protected by a firewall. In the rejection of claim 1, the Examiner asserts that the repository 12 in LAN 11 of Vaidya is the "client" recited in claim 1 and the collector 10 in the network 24 is the "server" recited in claim 1. This assertion is respectfully traversed. First, the repository 12 cannot be a client and the collector 10 in the network 24 cannot be a server. Vaidya defines in col. 1, lines 20-26 that a server is a service provider and a client is a customer of that service. In Vaidya, the central data repository 12 in the LAN 11 provides the service of storing network security data for the network 24. On the other hand, the collector 10 of the network 24 monitors the data coming into the network 24 but does not provide any service to the repository 12. Thus, in Vaidya, the repository 12 of the LAN 11 is a server, not a client, and the data collector 10 in the network 24 is a client, not a server, as asserted by the Examiner.

Second, the data collector 10 in the network 24 is not a "server protected by a firewall" as recited in independent claim 1 because the data collector 10 of the network 24 does not have a firewall. In the Final Office Action, the Examiner asserts that Vaidya discloses in the first paragraph of the detailed description (col. 5, lines 5-26), that data collectors 10 can be firewalls. *Office Action*, page 2. This assertion is improper because it is a misinterpretation of Vaidya. More particularly, Vaidya does not disclose that data collectors 10 could be firewalls. Rather, Vaidya discloses that although the data collectors 10 are shown as stand-alone devices, the function of a data collector can be "included" into other devices such as the server or router/firewall/switch 20. *Vaidya*, col. 5, lines 9-12. What that means is the function of the data collector 10 for the server 18 in the LAN 11 could be included into the server 18, and the function of the data collector 10 for the router/firewall/switch 20 could be included into the router/firewall/switch 20. *See Vaidya*, Fig. 1, server 18 and firewall 20. The disclosure in col. 5, lines 9-12 of Vaidya also means the function of the data collector 10 in the network 24 could be included into the work stations inside the network 24. However, the disclosure in col. 5, lines 9-12 does not mean that the data collector 10 by itself can be a firewall, as asserted by the Examiner. Therefore, the interpretation that all data collectors 10 in Vaidya can be firewalls, as asserted by the Examiner, is an unreasonable interpretation of the disclosure of Vaidya. As a result, it is respectfully submitted that the data collector 10 in the network 24 is not and cannot be a firewall for protecting the network 24. Therefore, Vaidya fails to teach a server in a second network protected by a firewall, as recited in independent claim 1.

In summary, Vaidya fails to teach or suggest a server in a second network protected by a firewall, and a query related to how the resources in the second network are used, as recited in independent claim 1.

Skonnard is cited in the rejection because Skonnard discloses the use of HTTP format to transport communications data from one network to another network through firewalls. Korematsu is cited in the rejection because Korematsu discloses in col. 1, lines 46-59 an authentication process between two parties where the first party sends an authentication request and the second party replies with an authentication acknowledgement. However, Skonnard and Korematsu each fail to teach or suggest a client party configured to send a query to another server party related to how resources in the network containing the server party are used, and the server party collects and sends that kind of data to the client party, as recited in independent claim 1. Therefore, Skonnard and Korematsu fail to cure the deficiencies of Vaidya. Accordingly, the proposed combination of Vaidya, Skonnard and Korematsu fails to yield all of the features of independent claim 1.

For at least the foregoing reasons, the Office Action has failed to establish that a *prima facie* case of obviousness against independent claim 1. Therefore, it is requested that the rejection of claim 1 be reversed and the claim be allowed.

Independent Claims 6 and 12:

Independent claim 6 recites a method in which the client sends at least one network usage query to the server, and the server collects and sends the network usage query to the client. Similarly, independent claim 12 recites a method in which the client sends at least one network configuration query to the server, and the server collects and sends the network configuration query to the client. Support for the "network usage query" recited in independent claim 6 and "network configuration query" recited in independent claim 12 can be found at least in paragraph [0015] of the specification of the present application. The "network usage query" recited in independent claim 6 and the "network configuration query" recited in independent claim 12 are the same as the query "related to how resources in the second network are used" recited in independent claim 1. Therefore, it is respectfully submitted that independent claims 6 and 12 are allowable over Vaidya in view of Skonnard and Korematsu for at least the same reasons set forth above with respect to independent claim 1.

At least for the reasons set forth above, it is respectfully submitted that the proposed combination of Vaidya in view of Skonnard and Korematsu fails to yield all of the features recited in independent claims 6 and 12. Accordingly, reversal of the rejection and allowance of independent claims 6 and 12 are respectfully requested.

Dependent Claims 2, 3, 7, 8, 11, 13 and 16-20:

Claims 2, 3, 7, 8, 11, 13 and 16-20 are dependent from allowable independent claims 1, 6 and 12. Therefore, these claims are also believed to be allowable over the cited documents of record for at least the same reasons set forth above with respect to independent claim 1. Reversal of the rejection and allowance of claims 2, 3, 7, 8, 11, 13 and 16-20 are respectfully requested.

B. The rejection of claim 10 under 35 U.S.C. §103(a) as being unpatentable over Vaidya in view of Skonnard, in view of Korematsu and further in view of Jackson should be reversed.

Claim 10 is dependent from allowable independent claim 6. As discussed above, the proposed combination of Vaidya, Skonnard and Korematsu fails to disclose all of the features of independent claim 6. In setting forth the rejection of claim 10, the Office Action has not and cannot reasonably assert that the disclosure contained in Jackson makes up for any of the deficiencies discussed above with respect to the proposed combination. Accordingly, even assuming for the sake of argument that one of ordinary skill in the art were somehow motivated to modify the proposed combination of Vaidya, Skonnard, and Korematsu with the disclosure contained in Jackson, the proposed modification would still fail to yield all of the features of independent claims 6.

For at least the foregoing reasons, the Office Action has failed to establish that claim 10 is *prima facie* obvious in view of the combined disclosures contained in Vaidya, Skonnard, Korematsu and Jackson, as proposed in the Office Action. Therefore, claim 10 is believed to be allowable over the cited documents of record for at least the same reasons set forth above with respect to independent claim 6. Reversal of the rejection and allowance of claim 10 are respectfully requested.

(8) Conclusion

For at least the reasons given above, the rejection of claims 1-43 described above and the objection to the Abstract described above should be reversed and these claims allowed.

Please grant any required extensions of time and charge any fees due in connection with this Appeal Brief to deposit account no. 08-2025.

Respectfully submitted,

Dated: July 2, 2009

By ______________________
Timothy B. Kang
Registration No.: 46,425

MANNAVA & KANG, P.C.
11240 Waples Mill Road
Suite 300
Fairfax, VA 22030
(703) 652-3817
(703) 865-5150 (facsimile)

(9) Claim Appendix

Claim 1. (Previously Presented) A network usage analyzer, comprising:

a network query client residing in a first network; and

a network query server residing in a second network protected by a firewall, wherein said network query client is configured to send authenticating information to the network query server, to send a query to the network query server related to how resources in the second network are used, wherein the network query server is configured to send authentication approval information to the network query client, to collect data related to how resources in the second network are used, and to send collected data to the network query client and wherein at least one query is formatted to enable transmission using Hypertext Transfer Protocol (HTTP) as the underlying transport mechanism.

Claim 2. (Original) The network usage analyzer, as set forth in claim 1, wherein the network query client and network query server are operable to communicate using a common protocol.

Claim 3. (Original) The network usage analyzer, as set forth in claim 1, wherein the network query client and network query server are operable to communicate using Simple Object Access Protocol.

Claim 6. (Previously Presented) A method for accessing information of resource usage in a first network, comprising:

establishing a communication channel between a network query client residing in a second network and a network query server residing in the first network protected by a firewall;

sending, by the network query client, authenticating information to the network query server;

sending, by the network query server, authentication approval information to the network query client;

sending, by the network query client, at least one network usage query;

receiving, by the network query server, at least one network usage query from the network query client, the at least one query formatted to enable transmission using Hypertext Transfer Protocol (HTTP) as the underlying transport mechanism;

collecting, by the network query server, information requested by the network usage query; and

sending, by the network query server, the collected information to the network query client.

Claim 7. (Original) The method, as set forth in claim 6, wherein establishing a communication channel comprises establishing a communication channel without reconfiguring the firewall.

Claim 8. (Original) The method, as set forth in claim 6, wherein establishing a communication channel comprises establishing a communication channel using Simple Object Access Protocol.

Claim 10. (Original) The method, as set forth in claim 6, further comprising:

periodically receiving, by the network query server, authenticating information from the network query client; and

sending, by the network query server, authentication approval to the network query client in response to the periodically received authenticating information.

Claim 11. (Original) The method, as set forth in claim 6, further comprising receiving, by the network query server, network configuration information.

Claim 12. (Previously Presented) A method for accessing information of resource usage in a first network, comprising:

establishing a communication channel between a network query client residing in a second network and a network query server residing in the first network protected by a firewall;

sending, by the network query client, authenticating information to the network query server;

sending, by the network query server, authentication approval information to the network query client;

sending, by the network query client, at least one network network configuration query to the network query server, the at least one query formatted to enable transmission using Hypertext Transfer Protocol (HTTP) as the underlying transport mechanism;

collecting, by the network query server, network configuration information requested by the network usage query;

receiving, by the network query client, information related to the network configuration query collected by the network query server; and

sending, by the network query server, the collected network configuration information to the network query client.

Claim 13. (Original) The method, as set forth in claim 12, wherein establishing a communication channel comprises establishing a communication channel using Simple Object Access Protocol.

Claim 16. (Previously Presented) The network usage analyzer, as set forth in claim 1, wherein the network query client transforms the usage data into business information.

Claim 17. (Previously Presented) The network usage analyzer, as set forth in claim 1, wherein the usage data comprises a metric measuring network usage levels based on at least one of a geographical region, a time of day, a particular user, and a type of service plan.

Claim 18. (Previously Presented) The method, as set forth in claim 6, further comprising, sending, by the network query server, the collected information to the network query client in order to transform the collected information into business information.

Claim 19. (Previously Presented) The method, as set forth in claim 12, further comprising transforming the collected information into business information.

Claim 20. (Previously presented) The method, as set forth in claim 12, further comprising sending, by the network query client, at least one network usage query to the network query service, the at least one network usage query requesting a metric measuring network usage levels based on at least one of a geographical region, a time of day, a particular user, and a type of service plan.

(10) Evidence Appendix

None.

(11) Related Proceedings Appendix

None.